Lab 9

Metasploit

Estimated time to complete: 30 Min

WHAT YOU WILL LEARN

You will learn how to use metasploit to find vulnerable devices and attack them.

Understanding metasploit can keep you ahead of the game whether you are on the CyberSecoffense or defense.

WHY IT'S IMPORTANT

Metasploit is used by whitehat and blackhat hackers to systematically probe and find exploits in networks and servers.

Metasploit also tells you the type of vulnerability your target equipment has, helping you to easily attack it or patch it.

SKILLS GAINED

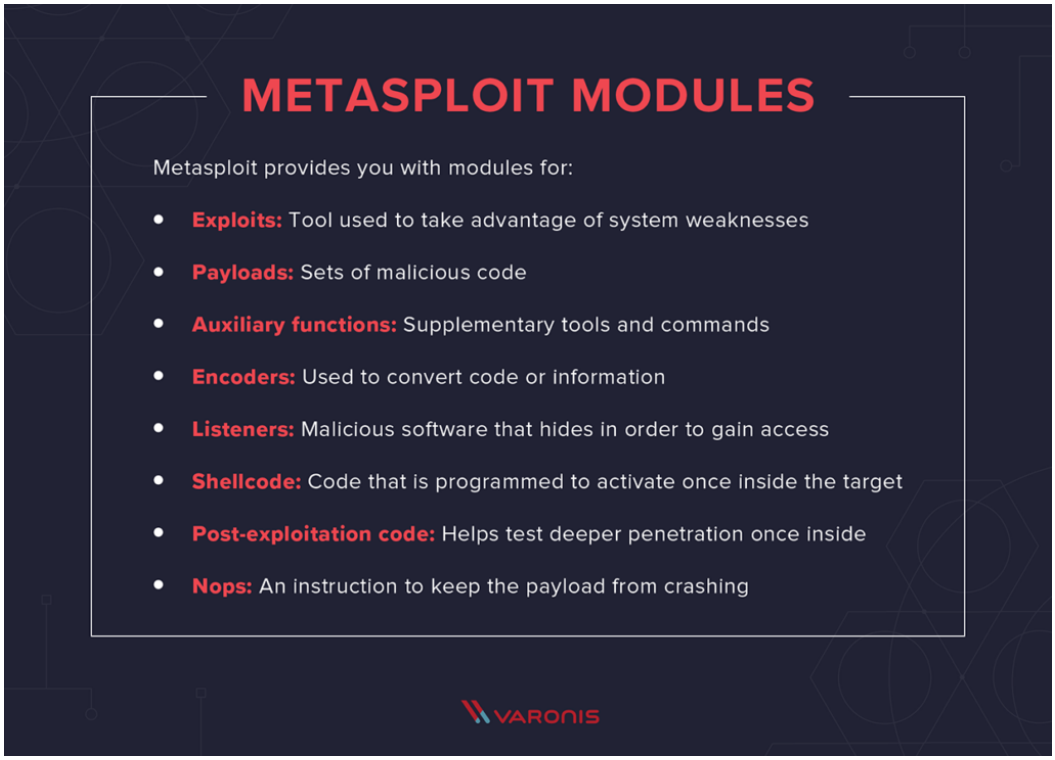
- Network scanning
- Penetration testing
- Service hardening

REQUIRED HARDWARE

- Raspberry Pi

WHAT IS METASPLOIT

Metasploit is a powerful tool that can be used to systematically probe for vulnerabilities on networks and servers. Metasploit contains over 1600 exploits on over 25 platforms including Linux, Windows, Android, Cisco and more. Once you find a vulnerable device, metasploit contains over 500 payloads that include a large variety of hacks and exploits. When combined with a powerful networking scanning tool like nmap, this might just be one of the most powerful tools in a hackers arsenal.

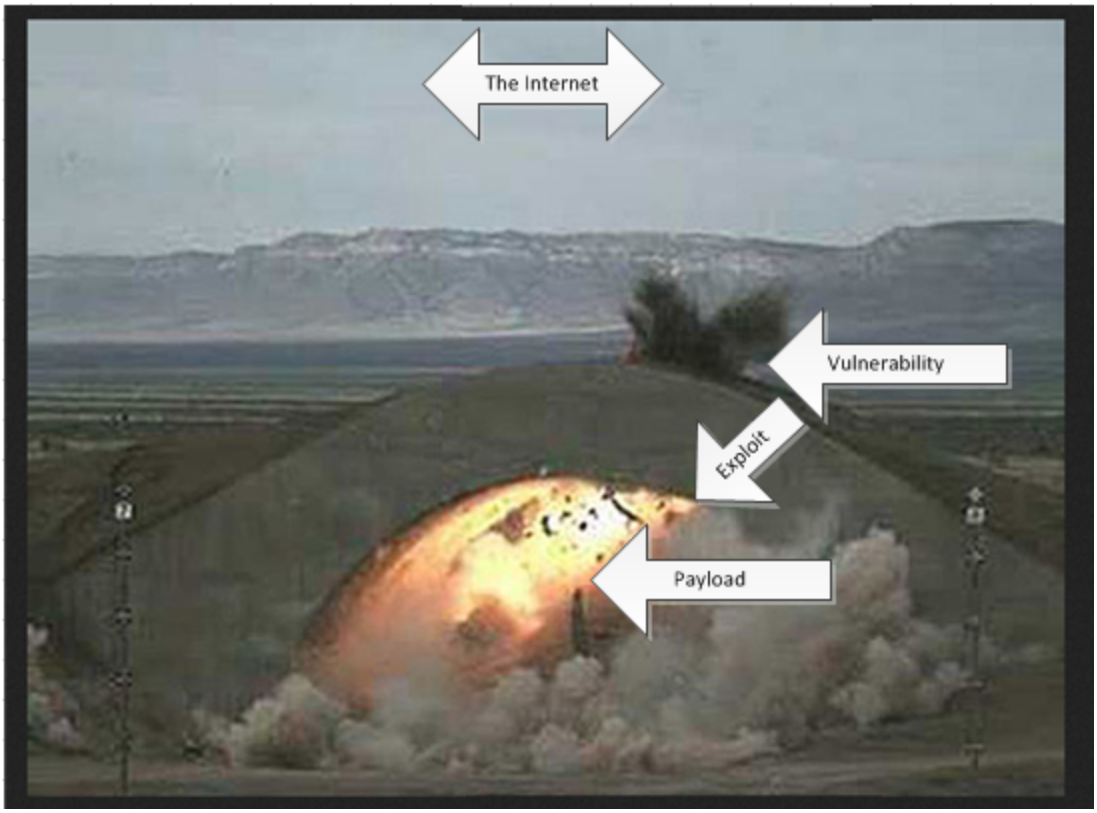


METASPLOIT FRAMEWORK VS PRO

Metasploit is available in two different editions: Framework and Pro. Framework is a free edition with a basic command-line interface and manual exploitation. The Pro edition is recommended for IT security teams and penetration testing as it has a multitude of advanced features for automation and infiltration such as smart exploitation, dynamic payloads, penetration testing reports, and many more. A comprehensive list of features can be found here: https://www.rapid7.com/products/metasploit/download/editions/.

EXPLOITS VS PAYLOADS

When learning metasploit, you will hear the terms vulnerability, exploit, and payload, it's important to know the difference. A **vulnerability** is a mistake in configuration or a fault in a technology that makes it exposed to attack, it's like a hole in the defenses of a network or system. How you decide to attack this vulnerability is the **exploit**, this can also be seen as the delivery system for the payload, common exploits may allow you to pop a shell or run your payload code where you normally wouldn't be able to. The **payload** is the piece of code that is actually doing damage, these can be things such as a rootkit, keylogger, trojans, RATs or reverse shells.



COMMON VULNERABILITIES AND EXPOSURES

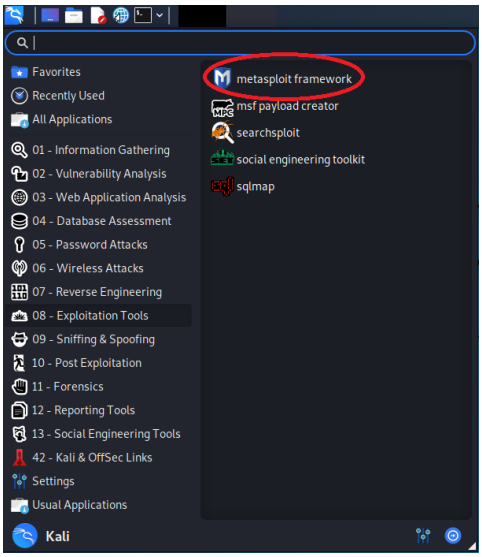
Common Vulnerabilities and Exposures, or CVE, is a long list of publicly known security threats and issues. This list is maintained by The Mitre Corporation and is sponsored by the US National Cyber Security Division of the US Department of Homeland Security. A vulnerability is a software coding error that allows hackers to directly access a system or network. An exposure is a software coding or configuration error that allows a hacker to indirectly access a system or network. CVE was designed to have a standardized way to identify vulnerabilities and exposures through the use of a CVE ID, allowing people to quickly reference the issue and find information about it.

BROWSING THE EXPLOITS

With over 1600 exploits, there's a lot to look at in metasploit. In this section we are going to look at all of the available common vulnerabilities and exposures and learn to navigate metasploit to find the right one.

STEP 1: STARTING METASPLOIT

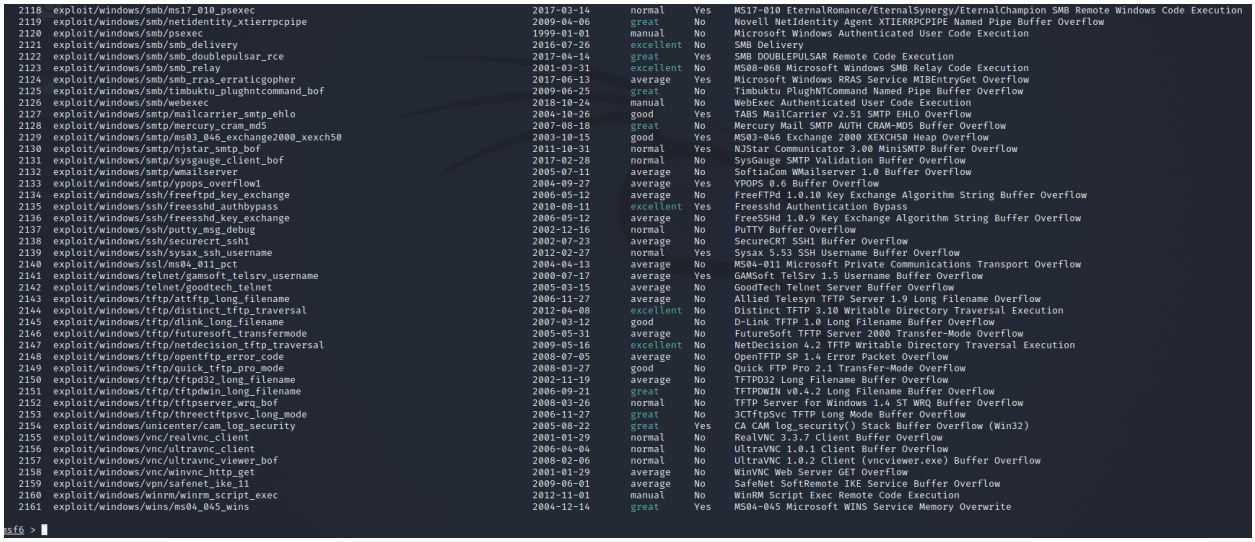
Open metasploit by clicking: Start Button -> "08 - Exploitation Tools" -> metasploit framework



Type in your password “*Pentesttheworld1!*” and hit enter in order to let the framework start

STEP 2: EXPLOITS AND PAYLOADS GALORE

Even though we are using the free version of metasploit, we still have access to a significant amount of exploits and payloads. You can look at the amount available to you on the start splash screen. In order to view all the exploits, we just need to type *“show all **exploits**”* and hit enter. You should see a screen similar to the one below:



Understanding this output may seem a little difficult, but it's pretty simple and helps us understand how searching works in metasploit. For example, take the exploit pictured here.:

Reading from left to right:

1323: This is the # of the exploit, this helps to keep track of an exploit but will only be unique to the search that we do.

exploit/windows/fileformat/adboe_flashplayer_button: This is the name of the exploit, this will not change between searches and can easily identify the exploit at a later time.

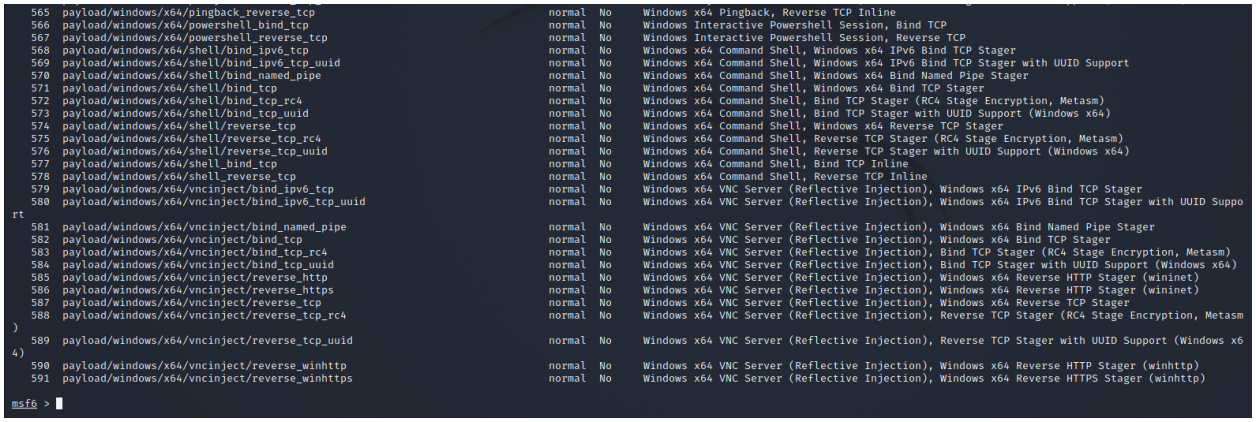
2010-10-28: This tells us what day the exploit was disclosed to the public.

normal: Normal defines the rank of the exploit. In this case, normal means that the exploit works but may need a specific version of the software and may have trouble auto detecting the service it is attacking

No: This tells us if the exploit is able to automatically "check" for the service on a target machine

Adobe Flash Player "Button" Remote Code Execution: This is the description of the exploit itself and can give users a quick glance as to what the code does.

Now that we understand the basic formatting of metasploit, we can also view all of the payloads



available on the free version using the command *"show all **payloads**"*

Take a few minutes and look at some of the payloads available and see if any of them could run on a device you own.

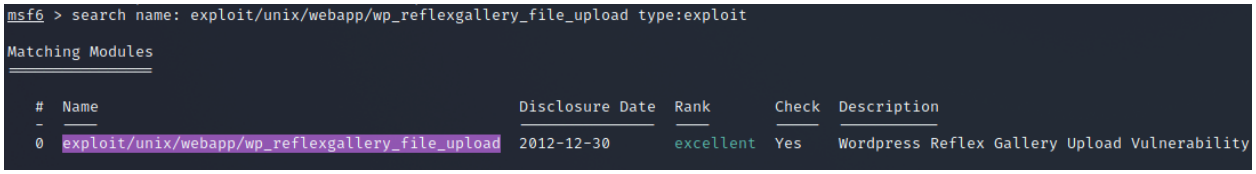
STEP 3: SEARCHING FOR SPECIFICS

While having all these exploits and payloads at the tip of your fingers is great, sometimes we want to get info on a specific exploit. In order to do this all we need to do is modify our search command. The layout of the command is

search name:[Exploit Name] type:[Exploit/Payload] platform:[Windows/Linux/Mac/Etc]

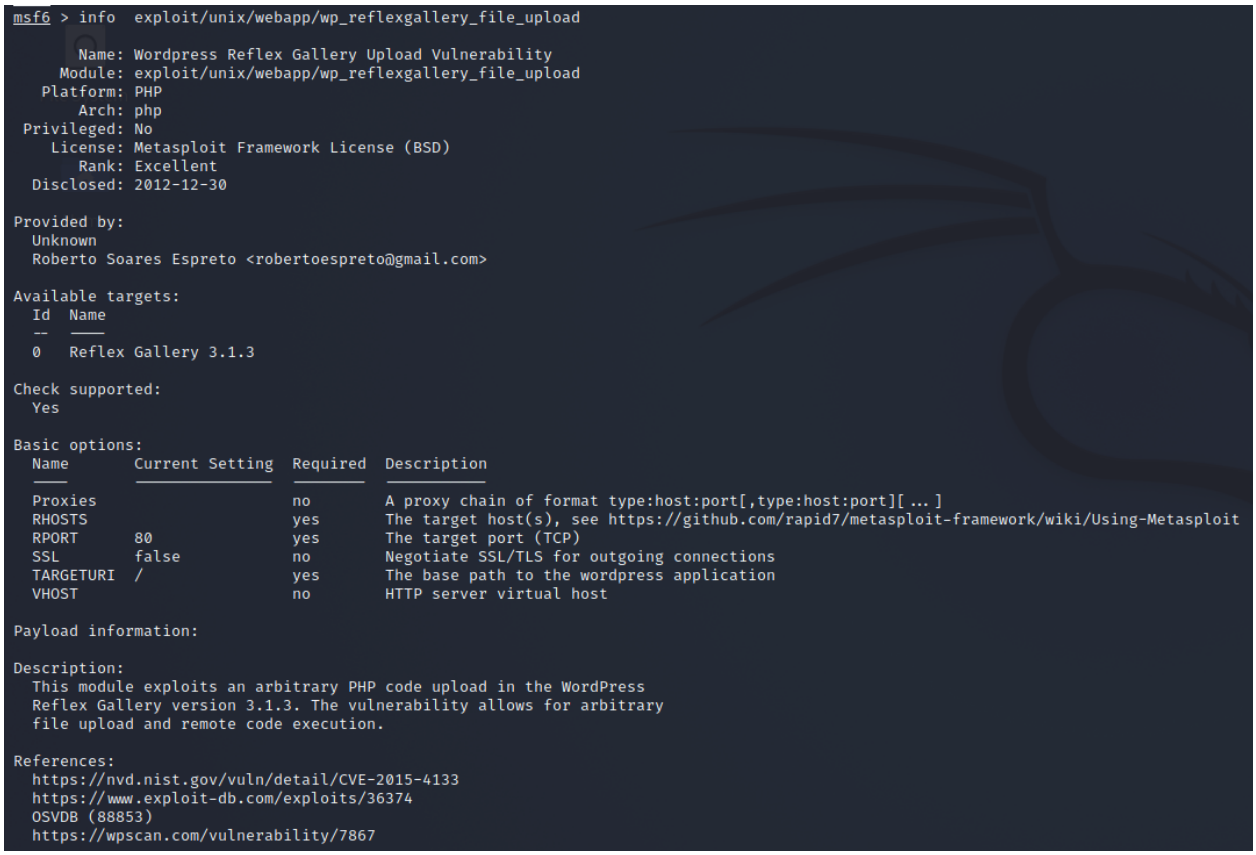
Using this, we can start looking for new vulnerabilities. Recently, we found out that a hacker used a wordpress upload exploit to run bad code on our servers. We think the name of the exploit is **exploit/unix/webapp/wp_reflexgallery_file_upload.** We can search for the exploit using the command below

"***search name: exploit/unix/webapp/wp_reflexgallery_file_upload type:exploit***"



Now we can see that is is real, we can find more information about the exploit using the command:

"info exploit/unix/webapp/wp_reflexgallery_file_upload"



Now we can see how it works, links to find more info at the bottom, and a description of all it's operations. From here, we can figure out how it did the exploit, and what services we should look at to stop it from happening again!

METASPLOIT CERTIFICATIONS

Metasploit has an online certification program called the Metasploit Pro Specialist Certification where you can become a certified pen-tester. The passing score is an 80 percent, the exam is online and open book which takes about 2 hours. It costs about $195 and you can print your certification once you've passed. There is also a metasploit training course that is directed toward those who do not have much cybersecurity or pen-testing experience and

should teach you everything you need to know to pass the exam, though it is very expensive, at around $2000 per student. The course will teach how to use metasploit pro, network scanning, exploitation techniques, web app testing, social engineering and reporting.

EXERCISES:

1: Tracing back the steps:

Uh, oh. Your boss just got hacked! He's really mad and wants to figure out what he did wrong to get hacked! One of the cybersecurity team members told him, his phone got hacked at home. They suspect his Netgear R7000 has malicious code running on it. Go check out the exploit "***exploit/linux/http/netgear_r7000_cgibin_exec***" and search the description to find what firmware version is affected by this.

2: Determine the vulnerability

Your firewall recently pick up two exploits running on the network. It seems one was blocked and the other one got through your security. Now all the Apple computers in the office talk whenever we highlight TEXT option. Look at these two exploits and determine which one got through so we can figure out how to stop it

post/osx/admin/say OR ***exploit/android/browser/samsung_knox_smdm_url***

REVIEW

1: What is an exploit?

A) A hole in the defenses of a network

B) How you deliver a payload

C) The code that does damage

D) A way to defend a hack

2: What is a CVE?

A) A metasploit version number

B) Common vulnerability environment

C) An index number for a certain known vulnerability

D) A mid 90s Honda

3: About how many vulnerabilities are available in metasploit?

A) 1600

B) 500

C) 150

D) 5000

4: What is **not** a feature in metasploit pro?

A) Smart exploitation

B) Dynamic payloads

C) Pen-testing reporting

D) AI brute forcing

5: Who is in charge of the CVE list?

A) Amazon Web Services

B) Mitre Corporation

C) Acme Corporation

D) US Department of Homeland Security

6: What is not an example of a payload?

A) A rootkit

B) A trojan

C) An open port

D) A keylogger

Answers: 1:B 2:C 3:A 4:D 5:B 6:C